التنظيـم القانوني للمسؤولية الدولية عن الجرائـم السيبرانية

م . د . عصام علي حسين
كلية القانون - جامعة الأمين

الكلمات المفتاحية: الجرائم السيبرانية.الأليات الدولية.المسؤولية الدولية.

الملخص:

إن مواجهة الجرائم السيبرانية تتطلب جهداً دولياً متكاملاً وشاملاً يشمل تطوير القوانين، تعزيز التعاون، والاستثمار في بناء القدرات التقنية والقانونية، ومع إن الطريق طويل ومعقد، فإن صياغة حلول قانونية مستدامة ستسهم في حماية الأمن الدولي وضمان العدالة لجميع الأطراف المتضررة من هذه الجرائم، ويبقى تحقيق التوازن بين حماية الخصوصية والسيادة الوطنية من جهة، وتعزيز الأمن السيبراني العالمي من جهة أخرى، هو التحدي الأكبر الذي يجب أن يواجهه المجتمع الدولي بحكمة ودقة.

المقدمة:

شهد العالم تطوراً هائلاً في التكنولوجيا واستخدام الإنترنت، ما أدى إلى ظهور الجرائم السيبرانية كأحد التحديات البارزة التي تواجه الدول والمجتمعات، فلم تعد هذه الجرائم تقتصر على الأفراد أو المؤسسات، بل أصبحت تشكل تهديداً للأمن الدولي والسيادة الوطنية، مثل الهجمات على البنية التحتية للدول أو التجسس الإلكتروني، وإنّ التعاون الدولي في مكافحة الجرائم السيبرانية يعد أمراً حيوياً في ظل التطور المتسارع للتكنولوجيا والانتشار الواسع لشبكة الإنترنت، يشمل هذا التعاون العديد من الالتزامات التي تضمن تنسيق الجهود وتبادل المعلومات بين الدول لمكافحة التهديدات السيبرانية.

أصبحت الهجمات السيبرانية أداة جديدة تتطلب اهتماماً فورياً في سياق السياسة الخارجية، فيتطلب التكييف السريع مع هذا التحول تطوير القدرات العسكرية والاستخبارات السيبرانية، لذلك قامت القوى الكبرى بتعديل استراتيجياتها السيبرانية حيث يُحدد أمانها الآن بشكل متزايد في الفضاء السيبراني، لذلك تُظهر الحاجة الملحة للتكيف مع هذا التحدي أنّ الأمان القومي ليس قائماً فقط على المواجهات العسكرية والاقتصادية والدبلوماسية، ولكن أيضاً يتم تحديده

بشكل كبير في الفضاء السيبراني، ويندرج العديد من التأثيرات السياسية والاستراتيجية تحت هذا الإطار مما يفرض الحاجة إلى استراتيجيات سياسية محددة لفهم الفضاء السيبراني كمجال جديد من الأمان والسياسة.

أمام هذه التحديات، برزت الحاجة إلى إطار قانوني دولي يُنظم المسؤولية عن الجرائم السيبرانية ويضع سبلًا لمعالجتها، ومع أن القانون الدولي يعالج المسؤولية عن الأفعال غير المشروعة بين الدول، فإن الطبيعة الخاصة للجرائم السيبرانية تستدعي تطوير أحكام وقواعد تتناسب مع هذا المجال الجديد.

أهمية البحث

تكمن أهمية هذه الدراسة من أجل:

1. البحث في السبل التي يجب اتباعها للتصدي لتلك الجرائم العابرة للحدود والتي تستلزم تحديد ماهيتها وخصائصها وطبيعتها وخصائص مرتكبيها وكيفية مساءلتهم.
2. تبيان مفهوم الهجمات السيبرانية وتكييفها قانونياً وتحديد الأليات التي قامت بها الدول من أجل التصدي لها ووالمبادرات في سبيل مكافحتها.

مشكلة البحث

إن الجرائم السيبرانية المستحدثة تمثل تحدياً دولياً لأي مجتمع بسبب المخاطر الناتجة عنها، فالتهديدات لم تعد تعتمد على قوة السلاح فقط، بل ظهرت وسائل إجرامية حديثة تعتمد على التقنيات الجديدة وعابرة للحدود، وهنا تكمن الإشكالية الرئيسية التالية:

ما مدى كفاية الأطر القانونية الدولية الحالية لمعالجة المسؤولية الدولية عن الجرائم السيبرانية؟ وكيف يمكن تطوير القانون الدولي ليواكب التحديات التي تفرضها هذه الجرائم؟

وتتفرع عن الإشكالية الرئيسية الأسئلة الفرعية التالية:

1. ما هي الطبيعة القانونية؟ وماهي الخصائص التي تميز الجرائم السيبرانية؟
2. ما هي آليات التعاون الدولي التي يمكن اعتمادها لتعزيز مكافحة الجرائم السيبرانية؟

فرضية البحث

على الرغم من غياب إطار قانوني دولي موحد وشامل للتعامل مع الجرائم السيبرانية، فإن القانون الدولي يوفر أدوات قانونية جزئية يمكن البناء عليها لتحميل الدول والجماعات الفاعلة

مسؤولية الجرائم السيبرانية، مما يستدعي تطوير آليات قانونية دولية فعالة لتحديد المسؤولية ومعالجة التحديات المتزايدة التي تفرضها هذه الجرائم على الأمن والسلم الدوليين.

هدف البحث

لقد قمنا بهذه الدراسة من أجل معرفة الأهداف التالية:

1. توضيح المسؤولية الدولية عن الجرائم السيبرانية من خلال دراسة كيفية تطبيق القانون الدولي الحالي على الجرائم السيبرانية، وتحديد الجهات المسؤولة عن ارتكابها.
2. تحليل الأطر القانونية الدولية وذلك عن طريق مراجعة الاتفاقيات والمعاهدات الدولية التي تتناول الجرائم السيبرانية أو التي يمكن تطبيقها عليها.

منهج البحث

لتحقيق أهداف الدراسة والإجابة عن الإشكالية المطروحة، تم اتباع المنهج الوصفي التحليلي من خلال وصف الجرائم السيبرانية وطبيعتها، وتحليل الأطر القانونية الدولية ذات الصلة، ودراسة النصوص القانونية مثل اتفاقية بودابست ومبادئ القانون الدولي العام.

خطة البحث

سوف يتم تقسيم هذه الدراسة إلى مبحثين، سنبحث في المبحث الأول مفهوم الجرائم السيبرانية. ونبحث في المبحث الثاني الآليات الدولية لمكافحة الجرائم السيبرانية.

ومن ثم خاتمة تتضمن أهم الاستنتاجات والتوصيات.

المبحث الأول:مفهوم الجرائم السيبرانية

تشير الجرائم السيبرانية إلى الأنشطة غير القانونية التي تُرتكب باستخدام الأنظمة الحاسوبية أو الشبكات الإلكترونية كوسيلة أو كهدف، وتشمل هذه الجرائم مجموعة واسعة من الأفعال، مثل اختراق الأنظمة، وسرقة البيانات، والاحتيال الإلكتروني، ونشر البرمجيات الضارة، والتجسس الرقمي، وانتهاك الخصوصية.

تُعتبر الجرائم السيبرانية تحدياً عالمياً متزايداً في ظل التطور التكنولوجي السريع واعتماد الأفراد والمؤسسات على الفضاء الرقمي في مختلف جوانب الحياة. وتتطلب مكافحة هذه الجرائم تعاونًا دوليًا وتشريعات صارمة وتقنيات متقدمة لحماية البنية التحتية الرقمية وضمان أمن المعلومات.

بناءً على ذلك سوف نقوم بتقسيم المبحث إلى مطلبين، سوف نتحدث في المطلب الأول عن تعريف الجرائم السيبرانية، أما في المطلب الثاني سوف نتحدث عن الطبيعة القانونية للجرائم السيبرانية.

المطلب الأول :تعريف الجرائم السيبرانية

تعددت التعريفات التي تناولت مصطلح الهجمات السيبرانية على ضوء الاجتهادات الفقهية، والممارسات العملية الدولية، فالهجمات السيبرانية مصطلح يستخدم من قبل فئات عديدة من الناس، للإشارة إلى أشياء مختلفة كالإشارة إلى وسائل القتال وأساليبه، تلك التي تتألف من عمليات في الفضاء الإلكتروني والتي يمكن أن ترتقي إلى مستوى النزاع المسلح، أو تُجرى في سياقه، ضمن المعني المقصود في القانون الدولي، فنذكر بعض أقوال فقهاء القانون الدولي من تعريفاتهم وتوجيهاتهم نحو الهجمات السيبرانية على ما يلي:

فعرفه البعض بقولهم: "هجوم عبر الأنترنت يقوم على التسلل إلى مواقع الكترونية غير مرخص بالدخول إليها، بهدف تعطيل أو إتلاف البيانات المتوفرة فيها أو الاستحواذ عليها، وهي عبارة عن سلسلة هجمات الكترونية تقوم بها دولة ضد أخرى[1]".

ومنهم من عرفه بأنه: "مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نظم المعلومات المعادية بهدف التأثير والإضرار بها، وفي الوقت نفسه للدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة"[2]، ومنهم من قال: "مجموعة من العمليات القائمة على الحرب السيبرانية والخداع النفسي، فضلاً عن استهداف شبكة تواصل العدو العسكرية وعملياته الأمنية الإلكترونية "[3].

مجموعة من المميزات والخصائص تتميز بها للجريمة السيبرانية، تميزها عن الجرائم التقليدية، وتحدد ما هيتها ووصفها الدقيق، مما يمكننا من التعرف على الظروف التي أدت إلى ظهورها وأشكال التي تظهر عليها والخسائر الناتجة عنها، ويمكن ملاحظة ما يميزها من خصائص، من خلال النقاط الآتية:

أولاً: خصائص الجرائم السيبرانية على الصعيد الوطني:

إن من سمات الجرائم السيبرانية أنها إحدى الجرائم المستحدثة، والتي تم تطويرها نتيجة التطور التكنولوجي الحاصل، وتغيّر أنماط الحياة ووسائل العيش، فهي وليدة التطور الذي شهدته الحياة المعاصرة، حيث استخدم مرتكبو هذه الجرائم التقنيات الإلكترونية الحديثة، في التحضير والتنفيذ وإخفاء أدلة الجرائم المرتكبة من أجل الهروب من الملاحقة القضائية، الأمر الذي يحفز على ارتكابها[4].

إن تزايد استخدام الانترنت، والقفزات النوعية في مجال التكنولوجيا الرقمية، جعلت التشريعات الجنائية التقليدية علي المستوى الوطني غير كافية لاستيعاب الأعمال غير القانونية الناتجة عن الأنشطة السيبرانية، فالتقدم السريع للتقنيات الحديثة، جعل من الجرائم التي

ترتكب بواسطتها خارج الإطار التشريعي التقليدي، المحكوم بالمبدأ الجزائي المعروف"لا جريمة ولا عقوبة إلا بنص" الأمر الذي جعل العقاب على الجرائم السيبرانية خارج الأنظمة الجزائية الوطنية التقليدية[5].

واللافت للنظر أن الآثار المرتبة على الجريمة السيبرانية، ذات قيمة مادية عالية بالنسبة للجرائم العادية التقليدية، وخاصة تلك التي تتعلق باستهداف البنوك والتحويلات المالية، الأمر الذي يلقي بظلاله ويتأثر به نسبة كبيرة من المجتمع المستهدف[6].

وبالتالي نظراً لخطورتها تتطلب هذه الجرائم استراتيجيات خاصة لمكافحتها، من خبرة وأدوات وأجهزة لتنفيذ القانون، ووعي من قبل المواطن لمخاطرها وشعوره بواجب التبليغ عنها في حال معرفته بإحداها[7]، وكذلك من الصعب قياس أو حصر الجرائم وتقدير حجم الخسائر الناتجة عنها لأسباب مختلفة، منها عدم وجود جهات رسمية لتوثيق الشكاوى وإصدار الإحصاءات الرسمية، وغياب جهات تحقيق متخصصة لكشف هذا النوع من الجرائم، بالإضافة إلى صعوبة تتبع أثر هذه الجريمة، وكذلك أدوات التحقيق وتعقب المتهمين، وأساليب مراقبة متطورة تحاكي الوسائل الحديثة التي ترتكب بها هذه الأنشطة[8].

ثانياً: خصائص الجرائم السيبرانية على الصعيد الدولي:

تجاوزت الجرائم السيبرانية نتيجة تطور وانتشار شبكة الإنترنت والاتصال عبر الأقمار الصناعية الحدود الجغرافية للدولة الواحدة، مما أتاح انتشار الجريمة عبر الشبكة، وأصبح العالم كله ساحة لها، فأخذت تتميز بكونها من الجرائم العابرة للحدود أي جريمة داخلية ينص عليها في القانون الداخلي تتضمن عنصراً ذا طابع دولي، تتعاون الدول في مواجهتها عن طريق الاتفاقيات الدولية، على اعتبارها تهديداً للنظام الدولي، ومبدأ العالمية في الفقه الجنائي الحديث يتطلب توحيد القواعد القانونية التي تحتويها نصوص التجريم في كل دولة، على اعتبار أن هذه الجرائم المستحدثة تمر بعدة أقاليم تابعة لعدة دول، فقد يتم ارتكاب الجريمة في إقليم، وتحدث نتيجتها في إقليم، وقد تكون الضحية من إقليم ثالث، مما يترتب عليه خضوعها للاختصاص العالمي وضرورة تعاون الدول على مكافحتها بقواعد قانونية دولية[9].

نستنتج مما تقدم إن الجرائم السيبرانية جرائم عابرة للحدود، تنتهك السيادة الإقليمية للدول، على اعتبار أنها في أغلب الأحيان، ترتكب في بلد، وتكون آثارها في بلد آخر، وذلك من قبل أشخاص لا ينتمون لكلا البلدين، حيث تعدد جنسيات الجناة في مثل هذا النوع من الجرائم، وكذلك تعدد أماكن ارتكابها يثير مسألة القانون واجب التطبيق عليها، وسبل وإجراءات

ملاحقتها، وأحقية القضاء المختص بالنظر فيها، الأمر الذي يصعب ملاحقة ومحاكمة مرتكبي هذه الجرائم.

ثالثاً: خصائص الجريمة السيبرانية المتعلقة بالجانب التقني:

من أهم ميزات الجريمة السيبرانية وقوعها في بيئة رقمية، وهذه الميزة تترتب عليها الكثير من الصعوبات على مستوى جمع الألة والإثبات والتحقيق، فقد اعتادت الأجهزة الأمنية التقليدية، على الأدلة المادية الملموسة، وبالتالي يصعب عليها البحث عن أدلة برمجية الكترونية، ونقلها من البيئة الرقمية إلى العالم المادي، واعتماد التحقيق على أساس برمجيات وأنشطة الكترونية، وبالتالي لا أدلة مادية في الجريمة السيبرانية، على عكس الجريمة التقليدية، لذلك تسمى جريمة ناعمة، حيث لا عنف ولا استخدام للقوة فيها، بل تتم بطرق فنية برمجية معقدة، دون أي مجهود عضلي، بعكس الجرائم التقليدية[10].

نلاحظ هنا أنه يتشرط في المجرم السيبراني أن يتميز بقدرات ومهارات عالية، فهو يعتمد على ذكائه ومهارته التكنولوجية ومواكبة أحدث التقنيات الرقمية وتعلمها واتقانها، لكي يستخدمها في عمليات اختراق الشبكات والقواعد الرقيمة والاستفادة منها أو اتلافها أو تغييرها، حسب ما يخدم مصلحته، والهدف الذي يعمل من أجله، وغالباً ما تكون أهداف المجرمين السيبرانيين مادية، بدافع كسب المال، أو أهداف شخصية، مثل انتقام موظف من الشركة أو المؤسسة التي كان يعمل بها، واستغنت عن خدماته، أو قد تكون أهداف عقائدية أو سياسية بتحريض من جهات رسمية أو غير رسمية[11].

كما تتصف الجريمة السيبرانية بأنها سريعة في التنفيذ، ينفذها الجاني بشكل مباشر أو من خلال البرامج الرقمية، بالإضافة إلى الصعوبة في اكتشافها، حيث تتم غالباً دون علم الضحية، كما يصعب إثباتها، وبالتالي ماهية الجريمة السيبرانية تختلف عن في الجريمة التقليدية اختلافاً جذرياً، حيث يصعب العثور على دليل مادي وإن اكتشف فيكون في الأغلب بمحض الصدفة، فمن الممكن على سبيل المثال حدوث جريمة فالتجسس السيبراني، بنسخ الملفات وسرقتها من الحاسوب، ومن النادر اكتشافها من قبل الشركات التي تقع ضحية لهما[12].

فضلاً عن أن الدليل غير المرئي عقبة كبيرة أمام كشف الجرائم السيبرانية، وسهولة محو هذا الدليل في زمن قصير يعد من الصعوبات التي تعترض عملية الإثبات في مجال إثبات هذه الجرائم، لأنه يسهل محو أدلة الإدانة وتدميرها في حالة تفتيش الشبكات أو عمليات التحقيق، وذلك في وقت متناهي الصغر[13].

كما تعتبر من أهم سمات الجريمة السيبرانية هي تطورها السريع وتجددها، ويظهر كل يوم طريقة جديدة وإسلوب جديد لارتكابها، لم تكن مألوفة من قبل، يرجع ذلك إلى التطور الهائل الذي تشهده تقنيات هذه الجرائم، فالجريمة تتطور على نحو يعجز عن متابعته الكثير من المختصين في هذا المجال[14].

كما أنها من الجرائم سهلة الارتكاب، فطالما توافرت لدى الفاعل الوسائل التكنولوجية لارتكاب الجريمة والتقنيات اللازمة، وأصبح من السهل ارتكاب الجريمة، الأمر الذي يبين بوجود خاصية أخرى إلا وهي كون هذه الجرائم تجذب المجرمين، فسهولة تحقيق المنفعة والمكسب المادي العالي وغياب النصوص العقابية لأغلب الجرائم يجعل منها جرائم مغرية[15].

وتدخل الهجمات السيبرانية في إطار الحرب الغير متكافئة وذلك كون الطرف الذي يتمتع بقوة هجومية ويبادر باستخدامها هو الطرف الأقوى، بغض النظر عن حجم قدراته العسكرية التقليدية، ولا تتطلب لتنفيذها سوى وقت زمني محدود، وتلعب المهارات البشرية دوراً أساسياً في تطويرها، كما يعد استخدام الأنشطة السيبرانية جزءاً من عمليات المعلومات المستخدمة في مستويات ومراحل الصراع المختلفة على الجانب التكتيكي أو الاستراتيجي ويتم ذلك بطرق عدة ومتنوعة وسريعة التطور[16].

نستنتج مما تقدم إن ما كان يعد من قبيل الخيال العلمي في الماضي أصبح حقيقة في الوقت الحاضر، فالجرائم تقع في بيئة رقمية، والأدلة التي تخلفها، تختلف عن الأدلة التي تتركها الجرائم التقليدية، فهي بلا آثار مرئية، ويمكن ارتكابها بسرعة نتيجة للتقنيات المستخدمة، كما أنها جرائم متطورة بتطور بيئتها قياساً بباقي الجرائم، وكما تتميز عمليات أو أنشطة الفضاء السيبراني بقلة تكاليفها وسهولة إخفائها والقدرة على التأثير على أهداف إلكترونية رقمية، مثل البنية التحتية الحيوية والمؤسسات الاقتصادية والمالية والسياسية والعسكرية، حيث يمكن صنع ترسانة سيبرانية وتجهيز المعدات الإلكترونية اللازمة لها، بقدر تكلفة دبابة حربية واحدة، بالإضافة إلى أن مصدرها يمكن أن يبقى مجهولاً ويمكن إنجاز الهجوم في زمن قياسي، دون معرفة الحجم الفعلي للخسائر، ولا يمكن معرفة الطريقة التي تمّ فيها الهجوم.

المطلب الثاني:الطبيعة القانونية للجرائم السيبرانية

وردت الهجمات في القانون الدولي بأنها أعمال العنف ضد الخصم سواء تم القيام بها على سبيل الهجوم أو الدفاع وبعيداً عن المنطقة التي تنفذ فيها تلك الأعمال، وهذا ما نص عليه البروتوكول الإضافي الأول لاتفاقيات جنيف لعام 1977[17]. وعلى وفق ما تقدم فإن التركيز على آثار النشاط

السيبراني وجسامته سببين إن وصف الهجوم متحقق فيه على سبيل المثال عندما تتعرض الحواسيب أو الشبكات في دولة ما للهجوم السيبراني، فقد يؤدي ذلك إلى حرمان المدنيين من الاحتياجات الأساسية كمياه الشرب والرعاية الطبية والكهرباء.

ويمكن أن تتدخل النشاطات السيبرانية في تعطيل خدمات إنقاذ الأرواح كالمستشفيات أو تعطيل البنية التحتية الحيوية مثل السدود والمفاعلات النووية وأنظمة التحكم في الطائرات، وجراء كل هذا قد يتضرر مئات الآلاف من السكان فمثل هذه النشاطات وعلى وفق جسامتها وآثارها سواء المباشرة منها أو غير المباشرة، تعد هجوماً سيبرانياً أي ينطبق عليها وصف (الهجوم) [18].

ومن ناحية أخرى كثيراً ما يتم اللجوء إليها لتنفيذ هجمات مسلحة تقليدية من خلال تعطيل اتصالات الخصم لتسهيل وحماية حركة السلاح الجوي لتنفيذ غارته وإلحاق الضرر بالعدو، أو يتم استخدامها لتحديد المواقع الحساسة لدى العدو ليتم قصفها وتدميرها.

أولاً: الهجمات السيبر انية وسيلة للقتال: إذا كانت الهجمات السيبرانية بذاتها تتسلل إلى أنظمة إلكترونية معدة للحماية أو تنظيم سير عمل منشآت حيوية للسيطرة عليها وتدميرها، فهنا تعد وسيلة للقتال أي سلاحاً تهاجم به العدو [19].

ومن أهم الإشكاليات التي تواجه المجتمع الدولي في طريقة التعامل مع الهجمات والجرائم السيبرانية هي ما يتعلق بالجدل حول إمكانية عد الأنشطة السيبرانية كسلاح وإمكانية خضوعها لقيود الاتفاقيات المعنية بالحد من التسلح، إذ ذهب بعض الخبراء بعدم صحة وصف الهجمات السيبرانية بأنها "سلاحاً" لأنها تفتقد إلى الطاقة الحركية، وبالتالي عدم خضوعها للتنظيمات الدولية المتعلقة باستخدام الأسلحة [20]، وهذا مخالف للواقع إذ لا يشترط في الأسلحة احتواؤها على الطاقة الحركية وخير مثال على ذلك الأسلحة الكيميائية أو البيولوجية، فحقيقة السلاح هي في كل ما يمكن أن يحدث ضرراً جسدياً أو مادياً، ويستعمل لغرض الدفاع أو الهجوم أو التهديد [21].

وقد أشارت اللجنة الدولية للصليب الأحمر عند حديثها عن الأسلحة السيبرانية أنّ تقييم مشروعية الأسلحة الجديدة يصب في مصلحة كافة الدول، حيث أنه يساعدها في ضمان توافق سلوك قواتها المسلحة مع الالتزامات الدولية، وبالإضافة لذلك تلزم المادة 36 من البروتوكول الإضافي الأول لعام 1977 كل دولة من الدول الأطراف التحقق من امتثال أي أسلحة جديدة تقوم تنشرها أو تدرس مسألة نشرها لقواعد القانون الدولي [22]، وهذه نقطة أخرى استحضرها دليل " تالين " على نحو مفيد.

ثانياً: الهجمات السيبرانية أسلوب للقتال: إذا أسهمت الهجمات السيبرانية في توجيه العمليات العسكرية وسهلت عمل القوة العسكرية التقليدية، فتعد أسلوب للقتال، كالطائرات بدون طيار Drawn التي توجه لتحيد أهداف عسكرية منتخبة، ومن ثم تدميرها للإخلال في صفوف القوة العسكرية المعادية، أو استخدام الهجوم السيبراني لإيقاف عمليات الاتصال في المطارات العسكرية والمدنية[23].

ففي هذه الحالات، لم يستخدم الهجوم السيبراني لتحقيق الهدف بنفسه بل لتمهيد الطريق أمام القوات العسكرية لتحقيق ميزة أو أفضلية عسكرية على العدو، فلذلك يمكن عدها طريقة قتالية وأسلوب قتال وإدراجها ضمن التخطيطات والتكتيكات العسكرية[24].

ومن الأمثلة على ذلك ما قامت به إسرائيل عام 2007 ضد سوريا، حيث لجأ سلاح الجو الإسرائيلي إلى استخدام تكنولوجيا متقدمة جداً تمكن بموجبها من اختراق منظومات الاتصال وأجهزة الرادار التابعة للقوات السورية، لمنع اكتشاف طائراتها، فظهرت السماء صافية في الرادارات السورية في الوقت الذي كانت تحلق طائرات إسرائيلية في المجال الجوي السوري وتقوم بتفجير وتدمير أهداف، كانت بناء على الاستطلاعات الإسرائيلية مشروعاً لإنشاء مركز ذات نشاطات نووية غير مدنية حسب ما ادعت إسرائيل بذلك [25].

ومثالاً آخر على ذلك هو ما قامت به روسيا عام 2008 ضد جورجيا حيث قام مخترقون محترفون من روسيا بإعادة توجيه الاتصالات بشبكة الإنترنيت من جورجيا إلى أجهزة خوادم في روسيا مما أدى إلى زعزعة نشاط الحكومة في جورجيا وتزامناً مع تلك الهجمات قامت روسيا بشن هجمات عسكرية على جورجيا [26].

أما موقف الفقه الدولي من للحروب السيبرانية، فهنا لابد أولاً من بيان التعريف الفقهي حول الحرب فقد عرفت الحرب بأنها حالة من الصراع العنيف الذي يقوم بين جماعتين سياسيتين مستقلتين عن طريق جيش منظم يسعى لتحقيق سياسة وطنية معينة ومن خلال ما سبق يمكن اعتبار الحرب بأنها حالة طبيعية تنشأ نتيجة وجود تناقض في المصالح بين الأفراد والمجتمعات والدول، والإنسان جزءاً لا يتجزأ من هذه الطبيعة، ويمكن تمييز الحرب كمفهوم والحرب كعملية، فالحرب كمفهوم قد يصف بأنها حالة قانونية فالحرب لا تتضمن فقط انتشار أعمال العنف المسلح بين أطرافها ويترتب على هذا المفهوم ضرورة التزام أطرافها باحترام القواعد التي حددها القانون الدولي [27].

لقد اختلف الفقه والقضاء الدولي[28] حول تحديد الوصف القانوني للهجوم بالفيروسات المعلوماتية على شبكات الاتصال، فهناك رأي وصف هذا الهجوم بأنّه عدوان تنطبق عليه خصائص الفعل العدواني، واتجاه آخر رأى عكس ذلك فالعدوان ومدى انطباقه على الحرب السيبرانية.

ومما سبق نرى أن هناك صعوبات كبيرة تواجه التكييف القانوني للهجمات السيبرانية في ظل قواعد القانون الدولي ككل، خاصة وأنه في ظل التطور التكنولوجي والتقني الذي أدى إلى انتشار استخدام الأسلحة السيبرانية سواء أكان بمفردها أم بالارتباط بأسلحة أخرى.

المبحث الثاني:الآليات الدولية لمكافحة الجرائم السيبرانية

تُعد الجرائم السيبرانية من التحديات الكبرى التي تواجه العالم في العصر الرقمي، حيث تتطلب مواجهتها تعاوناً دولياً وآليات فعّالة للتصدي لها، تتنوع هذه الآليات بين التشريعات الدولية الموحّدة، مثل اتفاقية بودابست لمكافحة الجرائم السيبرانية، وتعزيز التعاون بين الدول لتبادل المعلومات والخبرات.

كما تشمل الجهود إنشاء فرق استجابة سريعة للحوادث السيبرانية وتطوير برامج تدريبية لرفع كفاءة العاملين في هذا المجال، بالإضافة إلى ذلك تلعب المنظمات الدولية، مثل الإنتربول ومنظمة الأمم المتحدة، دوراً محورياً في تنسيق الجهود وتعزيز الالتزام بالمعايير الدولية، من المهم أن تستمر الدول في تحديث استراتيجياتها لمواكبة تطور التهديدات السيبرانية وضمان حماية البنية التحتية الرقمية العالمية. **بناء على ذلك سوف نقوم بتقسيم المبحث إلى مطلبين، سوف نتحدث في المطلب الأول عن سبل مواجهة الجرائم السيبرانية، أما في المطلب الثاني سوف نتحدث عن المبادرات الدولية في سبيل مكافحة الجرائم السيبرانية.**

المطلب الأول:سبل مواجهة الجرائم السيبرانية

مازالت الهجمات السيبرانية في الآونة الأخيرة سلاح فتاك استخدمته قوى مختلفة سعياً منها لتحقيق غايات محددة، هذا السلاح الذي يعتمد على فكرة الهجوم التكنولوجي الافتراضي أضحى اليوم أكثر خطورة يهدد أمن وسرية وخصوصية البيانات، فقد مس بأمن العديد من الدول وأسرارها حيث تعرضت العديد من الدول إلى اختراقات وقرصنة الكترونية خطيرة تمّ الفضح خلالها على أهم البيانات والخصوصيات التي تهدد أمنها، فالأمر أصبح أكثر صعوبة مما كان عليه سابقًا إذ أضحت كثير من المنظومات و المؤسسات في خطر فهي معرضة للاختراق من قبل هذه

الجهات الخطيرة التي تسعى إلى فضح أسرار وخصوصيات كبرى من شأنها الإطاحة بمنظومة معينة أو حتى دولة، وهذا ما سنتناوله من خلال التالي:

أولاً-مواجهة الإرهاب السيبراني:

هناك تحديات لمساعي مواجهة الإرهاب السيبراني، يتعلق كثير منها بالتطورات السريعة والمتلاحقة في مجال التقنية الالكترونية، وتطور برامج التخفي وعزل تقنيات التتبع، وتقدم برامج تغيير المواقع، لذا يمكن ترتيب سُبل مواجهة هذا النمط من الإرهاب وفق الاجراءات السياسية والتدابير التنظيمية الآتية [29]:

1-**السياسات السيبرانية**: إن سياسة الدولة على المستويين المحلي والدولي تحدد توجهاتها في الفضاء السيبراني، ويبدو أن بعض الدول الكبرى الناشطة في الفضاء الإلكتروني مثل الصين وروسيا لديها تحفظات تتعلق بهذا الفضاء، إذ رأت في العولمة السيبرانية تعدياً على سيادة الدولة القومية، ولا يمكن لأي دولة في ظلها أن تسيطر على المضمون المتداول بين مواطنيها عبر شبكة الإنترنت، لذلك أقامت كل منهما الحواجز اللازمة، وأنشأت شبكاتها القومية الخاصة ضمن إطار شبكة الإنترنت العالمية، وبحسب ضوابطها الخاصة، ونجحت كلا الدولتين في تحقيق ذلك، فضلاً عن تبني معظم الدول الكبرى الذباب الإلكتروني.

2-**تبادل التعاون المواجهة الكوارث والأزمات والمواقف الحرجة:** يمثل عنصر الوقت دورًا أساسيًا في المواقف الحرجة، ومن الأمور الحاسمة في مواجهة الأمر الذي يحتاج إلى تكثيف الجهود الخاصة والخبرات والإمكانيات بشكل يصعب تحقيقه إلا بتظافر الجهود الدولية، وهذا التعاون الأمني يمثل أهم الصور لمكافحة الجرائم السيبرانية الدولية، سيما وإنّ أجهزة العدالة الجزائية ليست بنفس المستوى والجاهزية في جميع الدول، وإنما هناك تفاوت فيما بينها، فبعض الدول المتقدمة تقنياً وتكنولوجياً لها دور كبير في مواجهة مثل هذه الجرائم تشريعياً وفنياً وبعضهم الآخر تفتقد لذلك، ومن هنا كان لابد من التعاون بين الدول[30].

نعتقد إن أهمية التعاون الدولي للحد من مخاطر الهجمات السيبرانية باعتبارها أحد الأخطار الحالية والمستقبلية على أمن الدول، لذلك إنّ التعاون بين جميع الدول في جميع المجالات يقلل من نسبة خطورة هذه الهجمات، لأن زيادة التعاون في مجال التدريب يعطي نتائج إيجابية لزيادة الثقة والوعي لرجال الشرطة والعدالة الجزائية.

3-**الجوانب التنظيمية والتشريعية**: إن التشريعات القانونية التي تراعي الجوانب الموضوعية والشكلية مهمة في مواجهة الإرهاب الإلكتروني على صعيد الدول، إذ يجب أن تنظم التشريعات

العمل في المجال الرقمي بإنشاء مؤسسات متخصصة بموجب قوانين خاصة، وتحديد طبيعة الجرائم والعقوبات الملائمة والرادعة لها، وشمول جميع الجوانب المتعلقة بالتجريم والعقوبات، والإجراءات الشكلية كالضبط والتحقيق والتوقيف وما شاكلها[31].

4-**الإستراتيجيات السيبرانية**: الإستراتيجية السيبرانية للدولة تحدد توجهها في هذا المجال، وتشمل كل السياسات والجوانب الأخرى ذات الصلة، مثل المؤسسات المخولة بتنظيم النشاطات الرقمية وضبطها، ومواكبة التشريعات للتطور الحاصل في هذا المجال، والاهتمام بتوعية المستخدمين بالمخاطر المحتملة.

5-**الاتفاقيات الإقليمية والتعاون الدولي**: تشمل الاتفاقيات الثنائية بين الدول الجوانب القانونية اللازمة للتعاون في مجال التحقيق في حوادث الفضاء الإلكتروني، أما التحالفات السيبرانية بين الدول، أو مع القطاع الخاص، فهي مهمة في عمليات التتبع والتحقيق في الحوادث، وتبادل المعلومات عن أبرز الطرق الإجرامية المتبعة، وأهم الأختام الرقمية والبصمات الإلكترونية الخاصة بالتنظيمات الإرهابية، وأحدث البرمجيات والأسلحة السيبرانية المستخدمة، ما يساعد على تحديد هوية الجهة التي تنفذ الهجمات الإرهابية السيبرانية، ويسهل استهدافها[32].

6-**إنشاء المجلس القومي للمعلوماتية والانترنت**: فالأمن المعلوماتي هو جزء حيوي من الأمن القومي، وان المسؤولية يجب أن يتعاون فيها كل من الجهات التقنية والأمنية والقضائية، على أن يكون من ضمن اختصاصاته اقتراح القواعد والتشريعات الخاصة بالمعلوماتية والانترنت وإعداد تقارير إحصائية ومتابعة ما تم عالمياً في هذا المجال[33].

7-**التدابير الأمنية والاستخبارية السيبرانية**:

تهدف إلى حماية الأنظمة والبنية التحتية الرقمية من التهديدات والهجمات السيبرانية. تشمل التدابير الأمنية الرئيسية كالوقاية، واكتشاف التهديدات، والنسخ الاحتياطي للبيانات، أما التدابير الاستخبارتية فتشمل الرصد والمراقبة وجمع المعلومات الاستخبارتية وتحليل البيانات.

لم يتفق بعض الخبراء في تحالف الدول العظمى مع الدول النامية في كل التفاصيل، أي لا ينبغي أن تفتح الدول العظمى مجالها الرقمي لهذه الدول، ولكنها تعمل للتعاون الجزئي، ويمكن أن تتحالف الدول كافة مع الشركات العاملة والبارزة في مجال الأمن السيبراني، ولا سيما الوطنية منها على أن يكون تعاونها بحسب قدرة الدولة على السيطرة على هذه الشركات، أما الشركات

الأجنبية التابعة للدول العظمى فيجب الحذر منها، والتعامل معها معاملة الدول الكبرى نفسها[34].

ثانياً-الاجراءات الفنية لمواجهة الهجمات السيبرانية:

أصبح التحقق من مدى مرونة أنظمة الدول أمرًا ضروريًا أكثر من أي وقت مضى، لضمان حماية بياناتها وتحديد مواطن الضعف لديها، والتي يمكن أن تشمل الأخطاء البرمجية أو اعتماد حواسيب أو إعدادات أمان غير كافية، حيث يمكن للقراصنة الذين يكتشفون هذه الثغرات غير المقصودة اغتنامها في تنظيم الهجمات السيبرانية المعروفة باسم هجمات يوم الصفر، ويتعين على مطوري البرمجيات إصدار التصحيحات البرمجية المحدثة لمواجهة هذه المشكلة، عوضاً عن اكتشاف هذه الثغرات بعد حصول الهجمة وفشلهم في إصلاح المشكلة وحماية المستخدمين[35].

تتضمن هذه الاجراءات تطوير البرمجيات والتطبيقات والأدوات والبنية التحتية الإلكترونية للدول لمواجهة الهجمات السيبرانية، وتشمل ما يأتي:

1-**تغيير الثقافة وتطوير التفكير السيبراني في المجتمع والتوعية الأمنية** تعد ضمن أبرز التحديات التي يجب العمل عليها، فضلًا عن نشر التوعية بين الأفراد لفهم المخاطر السيبرانية، مشيرًا إلى أنّ على الدول تقوم بدعم وتمكين مختلف الجهات في القطاع السيبراني[36].

2-**فهم الهجمات السيبرانية وكيفيتها وطريقة التعامل معها**، لأن مجال الأمن السيبراني يُعد من أخطر التحديات التي تواجه المنشآت والبيانات الالكترونية، إذ يجب العمل على تطوير أدواته داخل هذه المؤسسات لمواجهة الهجمات، فضلاً عن أهمية وجود خارطة طريق لموظفي الأمن السيبراني ومعرفة جميع الخطوط العريضة فضلاً عن وجود إستراتيجيات واضحة من شأنها أن تضمن استمرارية العمل والتطور للوصول إلى الأهداف السيبرانية[37].

3-**إنشاء جدران الحماية (Firewalls)**: لتكون خط الدفاع الأول للأنظمة والمعلومات، وهي برمجيات لحماية الأنظمة والبيانات وكشف الهجمات، وإجراءات أمن حسابات المستخدمين وطرق التحقق من الهوية تتضمن حماية الحسابات الرسمية والمصنفة، ويُعَدُّ الفرد هو العنصر الأهم في هذا الجانب، إذ على مديري الأنظمة وضع الوسائل الآلية واليدوية اللازمة للتحقق من هوية المستخدم[38].

المطلب الثاني:المبادرات الدولية في سبيل مكافحة الجرائم السيبرانية

على الرغم من تزايد الهجمات السيبرانية والخطورة الناشئة عنها، إلا إن المجتمع الدولي يفتقر إلى إطار قانوني دولي شامل ينظم هذا الموضوع، ومع ذلك فهو امر لا يعني صحة القول بعدم وجود

جهود دولية لتنظيم الهجمات السيبرانية بشكل مطلق، إذ هناك جهود تقدم بعض السبل التي يمكن توظيفها للسيطرة على هذا التهديد المتنامي [39]، وعليه سنتناول هذا المطلب على النحو الآتي:

أولاً: الأمم المتحدة:

أقرت الأمم المتحدة عدة قرارات بشأن التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي، وأكدت من خلالها على ما يلي: "قد تستخدم هذه التقنيات لأغراض تتعارض مع السلم والأمن الدوليين " وأيضا على أن انتشار البيانات واستعمال التقنيات والأساليب المعلوماتية قد تؤثر على مصالح المجتمع الدولي[40].

إلا إن هذه القرارات جاءت غامضة ولا تتطلب أية إجراءات محددة من قبل أعضاء الأمم المتحدة، ومن أمثلة القرارات الصادرة عن الجمعية العامة يمكن الإشارة إلى القرار المتعلق بـ إنشاء ثقافة عالمية بشأن الأمن السيبراني وحماية البنية التحتية الأساسية المعلومات"، وكذلك القرار المتعلق بـ إنشاء ثقافة عالمية بشأن الأمن السيبراني والاستفادة من الجهود الوطنية لحماية البنية التحية الأساسية للمعلومات، وعقد اجتماع دولي للخبراء في جنيف عام 1999 برعاية الأمم المتحدة يهدف إلى فهم أفضل للآثار الأمنية الناشئة عن تكنولوجيا المعلومات[41].

إن روسيا والولايات المتحدة الأمريكية تمثلان وجهات نظر متعارضة بشأن الأمن السيبراني فيما يتعلق بالسيادة والمعارضة السياسية، فضلاً عن التعاون الدولي، وإن الصراع الدائر بينهم يعيد مفهوم الهيمنة من أجل النفوذ وتحقيق كل منهما مكاسب محددة سلفاً قبل الخوض في مسألة تنظيم الهجمات السيبرانية بصيغة اتفاقية متعددة الأطراف، لذلك فإن التوصيات التي دعا إليها خبراء الأمن السيبراني تمثل تقدم حقيقي في التغلب على الجمود الممتد بين الولايات المتحدة وروسيا بشأن كيفية معالجة قضايا الأمن السيبراني[42].

إن التعاون الدولي هذا يوحي بإمكانية عقد معاهدة متعددة الأطراف في المستقبل تحت رعاية الأمم المتحدة والتي تعد روسيا من أهم المنادين بها وبالفعل هناك محادثات بشأن كيفية عمل معاهدة تنظم الهجمات السيبرانية بين الولايات المتحدة وروسيا، وإن كانت هذه المحادثات في مراحلها الأولية إلا إنها مشجعة[43].

ثانياً: دليل تالين بشأن تنظيم الهجمات السيبر انية:

هو وثيقة قانونية دولية بارزة أُعدت لتقديم إرشادات حول كيفية تطبيق القانون الدولي في الفضاء السيبراني، وخاصة في سياق الهجمات السيبرانية. أُعد هذا الدليل تحت إشراف "مركز

التميز للدفاع السيبراني التعاوني" التابع لحلف شمال الأطلسي (الناتو) في مدينة تالين، إستونيا، ويهدف إلى توضيح كيفية تعامل الدول مع الهجمات السيبرانية سواء في أوقات السلم أو النزاع المسلح [44].

بعد الهجمات السيبرانية التي استهدفت إستونيا في عام 2007، والتي نُظر إليها كأحد أولى الحروب السيبرانية الكبرى، ظهرت الحاجة إلى قواعد قانونية لتنظيم هذا النوع من النزاعات، جاء دليل تالين لتقديم إطار قانوني شامل يحدد كيفية تطبيق قوانين الحرب (مثل اتفاقيات جنيف) والقانون الدولي الإنساني على النزاعات في الفضاء السيبراني.

وإن دليل تالين (2013): ركز على تطبيق القانون الدولي أثناء النزاعات المسلحة السيبرانية، وشمل 95 قاعدة قانونية تتعلق باستخدام القوة، والسيادة، وحقوق الدول في الدفاع عن النفس ضد الهجمات السيبرانية. [45]

ودليل تالين (2017): توسع ليشمل الأنشطة السيبرانية في وقت السلم، مع الإشارة إلى القوانين الدولية التي تنظم العلاقات بين الدول في الفضاء السيبراني، كما ناقش مواضيع مثل المسؤولية القانونية للدول، الهجمات السيبرانية التي لا تصل إلى مستوى النزاع المسلح، وحماية البنية التحتية الحيوية [46].

ثالثاً: مبادرات منظمة شنغهاي للتعاون:

يعتبر إعلان يكاترينبورغ، الذي صدر في 16 يونيو 2009، من أبرز المبادرات التي قامت بها هذه المنظمة لتعزيز التعاون في مجال الأمن السيبراني، حيث أكدت الدول الأعضاء في منظمة شنغهاي للتعاون على أهمية ضمان أمن المعلومات الدولي كأحد العناصر الأساسية لنظام الأمن الدولي المشترك.

خلاصة القول إن الجهود المذكورة تبرهن على الاهتمام الدولي المتزايد لوضع أطر تنظيمية دولية لمعالجة الهجمات السيبرانية، هذه الجهود وان لم ترق إلى مستوى إطار تنظيمي دولي شامل على غرار القواعد التي تنظم النزاعات المسلحة التقليدية، إلا إنها تعد الخطوة الأولى نحو اتفاقية متعددة الأطراف تنظم استخدام هذه الهجمات وتقلل من آثارها الجسيمة على البشر [47].

رابعاً: مدى إمكانية تطبيق المادة (51) من ميثاق الأمم المتحدة على الهجوم السيبراني:

لا تزال القوة عنوان العلاقات الدولية حيث كان استخدام القوة في شن الحروب أمراً مشروعاً وإحدى الوسائل المستخدمة من أجل فض النزاعات بين الدول. قبل ميثاق الأمم المتحدة وميثاق عصبة الأمم كانت الدول تلجأ إلى القوة لشن الهجوم لأن القوة تعتبر مظهراً من مظاهر سيادة

الدول، حيث استطاعت الجهود الدولية في منظمة الأمم المتحدة إلى تغيير بعض القواعد التي كانت سائدة في عهد عصبة الأمم والتي منها استخدام القوة، حيث بات الأصل حظر استخدام القوة في العلاقات الدولية والاستثناء هو استخدامها في حالة الدفاع الشرعي مع تشيدها بالعديد من القيود وفقا للمادة (51) من ميثاق الأمم المتحدة [48].

استناداً لهذه المادة فإن كل دولة تتعرض للعدوان يكون من حقها الرد باستخدام وسائل القوة اللازمة لمواجهة العدوان فقط، ولا يجوز لها أن تتعدى في ذلك. لذا فإن الدفاع الشرعي ليس حق مطلق للدول بل مقيد ببعض القيود فلا يمكن استخدامه إلا إذا كان مستوفيا الشروط المنصوص عليها في المادة (51) من الميثاق [49].

لقد أصبحت مسألة أمن الفضاء السيبراني من أولويات الأمن القومي للعديد. من الدول التي تعتمد بشكل كبير على التكنولوجيا والاتصالات في إدارة شؤونها الداخلية، كما أن حق الدولة المعتدى عليها في الرد على الهجوم السيبراني يجب أن لا يخرج عن إطار ميثاق الأمم المتحدة والقانون الدولي الإنساني من حيث الضرورة والتناسب ويجب أن يستوفى رد الفعل في الدفاع عن النفس ضد الهجمات السيبرانية التي ترتقي إلى مستوى الهجوم المسلح بمتطلبات الضرورة والتناسب التي لم تشر إليه المادة (51) من ميثاق الأمم المتحدة بشكل واضح، إلا ان الرأي الاستشاري بخصوص الأسلحة النووية عام 1996 هو ان يتوفر في ممارسة الحق في الدفاع عن النفس شروط الضرورة والتناسب التي تعد قاعدة من قواعد القانون الدولي العرفي، حيث ان هذا الشرط المزدوج ينطبق على المادة (51) من الميثاق بغض النظر عن وسائل القوة المستخدمة. كما أن مسألة الضرورة تعد من الموضوعات الشائكة وتقييمها صعب للغاية لكن تطبيقاً لهذا المبدأ أن تكون القوة المستخدمة في الرد السبيل الوحيد المواجهة الدولة المعتدية. كما يجب أن يكون الرد على الهجوم السيبراني ضرورياً لكي يكون الرد قانونياً ينطبق عليه صفة الدفاع الشرعي [50].

إن حق الدولة المعتدى عليها في استعمال القوة للرد على الهجوم لا يكون مطلق وانما مقيد وفق المادة (48) من الملحق الإضافي لاتفاقية جنيف التي حددت الأهداف التي من الممكن استهدافها من الدولة المعتدى عليها وهي الأهداف العسكرية [51].

كما بينت اتفاقية لاهاي الرابعة أنه ليس من حق الدولة المعتدى عليها استهداف أو تدمير ممتلكات المدنيين وإلا عد استهدافها انتهاك لأحكام اتفاقية لاهاي مما يشكل جريمة وفقاً لأحكام اتفاقية روما المنشئة للمحكمة الجنائية الدولية.

وقد أكدت الإدارة الأمريكية على أن استخدام القوة في الدفاع عن النفس ضد أي هجوم سيبراني ينبغي أن يقتصر الرد على ما هو ضروري لمواجهة الهجوم. وكذلك أن يكون متناسباً مع الخطر الذي يواجه المواقف لان هذا بعد جوهر الدفاع عن النفس. وكذلك أكدت محكمة العدل الدولية في العديد من المواقف إن الدفاع عن النفس يجب ان يكون متناسباً مع الهجوم المسلح والضروري للرد باعتبارها قاعدة راسخة في القانون الدولي العرفي التي غابت عن احكام ميثاق الأمم المتحدة الخاصة في الدفاع عن النفس [52].

حيث يتوجب على الدولة التي تستخدم حقها في الدفاع عن النفس رداً على الهجوم السيبراني ان تلتزم بأحكام اتفاقية جنيف التي تمنع ان يتضرر السكان المدنيون وممتلكاتهم من جراء الأخطار الناجمة عن الهجوم المسلح، كما يجب ان لا تكون ممتلكات ومصالح المدنيين من بنوك ومستشفيات وكهرباء هدف للدولة صاحبة الحق في الرد لكي لا يكون حق استخدام القوة في الدفاع عن النفس من الدولة المعتدى عليها ذريعة لتدمير البنية التحتية للدولة المعتدية، حيث ان أي انتهاك لاتفاقية جنيف من قبل الدولة عند استعمالها حق الدفاع الشرعي ستكون مسؤولة عن هذا الانتهاك. لذلك فإن الدولة المعتدى عليها في حال استعمال حقها في مواجهة الهجوم السيبراني لم تراعي احكام اتفاقية جنيف واتفاقية لاهاي الرابعة سوف تتسبب في انتهاك احكامهما، لذلك فإن سوء استخدام القوة في الدفاع عن النفس قد يحول الدولة من صاحبة حق إلى دولة مسؤولة عن الانتهاكات التي خلفها الهجوم المخالف للأحكام والاعراف الدولية وعليه يجب ان يكون مبدأ التناسب حاضراً في كل الحالات لأنه يعد جوهر وروح القانون الدولي الإنساني [53].

ومن أهم الأمثلة على ذلك الهجوم السيبراني الذي تعرضت له مواقع الكترونية في استونيا عام 2007 الذي وصفه خبراء في أمن شبكات الكمبيوتر بأنه الأعنف في التاريخ، حيث استهدف البنية التحتية الإلكترونية بشكل كامل مما جعل استونيا معزولة عن العالم. وقد أكد خبراء في هذا المجال ان روسيا هي من تقف وراء هذا الهجوم المدمر، وكذلك الهجوم السيبراني الذي استهدف مفاعل النووي الايراني في عام 2010، حيث اتهمت إيران الولايات المتحدة الأمريكية واسرائيل بإرسال فيروساً الكترونياً أطلق عليه اسم (**Stuxnet**) الذي تسبب في تعطيل آلاف الحواسيب، كما استهدف أجهزة الطرد المركزي بهدف تعطيله.

الخاتمة

تُعد الجرائم السيبرانية من أبرز التحديات القانونية والأمنية التي تواجه العالم اليوم، فهي جرائم تتسم بالطابع غير التقليدي، حيث تستغل الفضاء الإلكتروني لتعبر الحدود الجغرافية، مما يجعل مواجهتها مسؤولية مشتركة بين الدول والمجتمع الدولي. ورغم أن القانون الدولي يتضمن مبادئ عامة تُنظم المسؤولية الدولية عن الأفعال غير المشروعة، فإن الطبيعة الفريدة للجرائم السيبرانية فرضت الحاجة إلى تطوير هذا الإطار القانوني. من خلال هذه الدراسة، تم التطرق إلى تحديات تطبيق المسؤولية الدولية على الدول والأفراد في الجرائم السيبرانية، مع التركيز على أهمية تعزيز التعاون الدولي وسن تشريعات شاملة لمواجهة هذه الظاهرة المتنامية. وفي نهاية الدراسة توصلنا إلى العديد من الاستنتاجات والمقترحات التالية:

أولاً_ الاستنتاجات

1. غياب إطار قانوني دولي شامل على الرغم من وجود بعض الاتفاقيات إلا أن القانون الدولي لا يزال يفتقر إلى إطار شامل يُنظم الجرائم السيبرانية بشكل موحد.
2. تحديات إثبات المسؤولية حيث إن الطبيعة التقنية المعقدة للجرائم السيبرانية تُصعّب من إثبات المسؤولية، سواء على الأفراد أو الدول، خصوصاً مع استخدام تقنيات مثل التشفير وإخفاء الهوية.
3. تُعقّد الجرائم السيبرانية مسألة الاختصاص القضائي، حيث يمكن أن يرتكب الجاني الجريمة من دولة بينما تكون آثارها في دولة أخرى.
4. التعاون بين الدول في مجال مكافحة الجرائم السيبرانية لا يزال محدوداً، بسبب تضارب المصالح السياسية أو ضعف البنية التحتية القانونية في بعض الدول.
5. الجرائم السيبرانية تُهدد الأمن القومي للدول، وتسبب خسائر اقتصادية هائلة، وتؤثر بشكل مباشر على خصوصية وأمن الأفراد.

ثانياً_ المقترحات

1. إبرام معاهدة دولية شاملة: ضرورة صياغة معاهدة دولية ملزمة لجميع الدول تتناول بشكل شامل الجرائم السيبرانية، تُحدد المسؤولية الدولية، وتضع آليات واضحة للتعاون في التحقيقات والمحاكمات، كتبادل المعلومات الاستخبارتية، وتسهيل التحقيقات الدولية، والتعاون في تعقب المجرمين وإنشاء محكمة خاصة بالجرائم السيبرانية.
2. تعزيز التعاون بين الدول من خلال تبادل المعلومات حول التهديدات السيبرانية.

3. إنشاء قاعدة بيانات دولية للهجمات السيبرانية لتتبع الجناة وتطوير استراتيجيات الوقاية.
4. حث الدول على تطوير قوانينها الوطنية لتتوافق مع المعايير الدولية لمكافحة الجرائم السيبرانية، وضمان قدرة الأنظمة القضائية على ملاحقة الجناة.
5. دعم الدول النامية بتطوير بنيتها التحتية الرقمية والقانونية لمواجهة الجرائم السيبرانية.

الهوامش:

---

[1] إسماعيل محمود الرزاز، الحماية القانونية من الهجمات والجرائم السيبرانية، مركز المحمود لتوزيع الكتب القانونية، مصر، 2023، ص17.

[2] علي محمد كاظم الموسوي، المشاركة المباشرة في الهجمات السيبرانية، المؤسسة الحديثة للكتاب، بيروت، 2019، ص21.

[3] احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، **مجلة المحقق الحلي للعلوم القانونية** والسياسية، كلية القانون، جامعة بابل، العدد 4، العراق، 2016، ص614.

[4] عبد الكريم الردايدة، الجرائم المستحدثة واستراتيجية مواجهتها، الطبعة الأولى، منشورات دار حامد للنشر والتوزيع، عمان، الأردن، 2013، ص 28.

[5] جمال إبراهيم الحيدري، الجرائم الإلكترونية وسبل معالجتها، منشورات مكتبة السنهوري، بغداد، 2012، ص 33.

[6] ذياب موسى البداينة، الجرائم المستحدثة في ظل المتغيرات التحولات الإقليمية والدولية، بحث مقدم إلى الملتقى العملي في كلية العلوم الاستراتيجية، عمان، الأردن، 2014، ص19.

[7] طارق عثمان، المركز الوطني للاستجابة لطوارئ الحاسب الآلي، صحيفة الدستور، العدد 12، مصر، 2012، ص213.

[8] مايكل شميت، الحرب بواسطة شبكات الاتصال الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب، المجلة الدولية للصليب الأحمر، بيروت، مختارات من أعداد 2012، ص 9.

[9] جمال إبراهيم الحيدري، مرجع سابق، ص 34.

[10] جمال إبراهيم الحيدري، المرجع نفسه، ص 36.

[11] تميم عبد الله التميمي، الجرائم المعلوماتية في الاعتداء على الأشخاص، الطبعة الأولى، منشورات مكتبة القانون والاقتصاد، الرياض، 2016، ص 16.

[12] طارق إبراهيم الدسوقي عطية، عولمة الجريمة، الشركات العالمية في الممارسات الإجرامية، دار الجامعة الجديدة، الإسكندرية، مصر، 2010، ص 230.

(13) جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، 2012، ص4.

(14) رايز بن سالم الحقباني، مهارات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه مقدمة إلى جامعة نايف للعلوم الأمنية، الرياض، 2013، ص 33.

(15) جلال محمد الزغبي وأسامة أحمد المناعسة، جرائم تقنية المعلومات الإلكترونية، الطبعة الأولى، منشورات دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010، ص 93.

(16) المرجع نفسه، ص 95.

(17) البروتوكولان الإضافيان إلى اتفاقية جنيف لعام 1949.

(18) إسماعيل محمود الرزاز، الحماية القانونية من الهجمات والجرائم السيبرانية، مركز المحمود لتوزيع الكتب القانونية، مصر، 2023، ص39.

(19) أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية، ط1، منشورات زين الحقوقية، بيروت، 2018، ص 21.

(20) زهراء عماد محمد، المسؤولية الدولية الناشئة عن الهجمات السيبرانية، مكتبة القانون المقارن، العراق، 2021، ص 31.

(21) محمود ابراهيم عبد الرحمن، أسلحة غير التقليدية في الفقه الإسلامي، أطروحة دكتوراه، كلية الشريعة والقانون، الجامعة الإسلامية، غزة، 2007، ص 7.

(22) المادة(36) من البروتوكول الإضافي الأول لعام 1977.

(23) عادل عبد صادق، أسلحة الفضاء الالكتروني في ضوء القانون الدولي الإنساني، مكتبة الإسكندرية، الإسكندرية، 2016، ص135.

(24) يحي مفرح الزهراني، الأبعاد الاستراتيجية والقانونية للحرب السيبرانية مجلة البحوث والدراسات، جامعة الوادي، العدد 23 ، 2017، ص 242.

(25) زهراء عماد محمد، المسؤولية الدولية الناشئة عن الهجمات السيبرانية، مرجع سابق، ص 33.

(26) زهراء عماد محمد، المرجع نفسه، ص34.

(27) عادل عبد صادق، أسلحة الفضاء الالكتروني في ضوء القانون الدولي الإنساني، مرجع سابق، ص139.

(28) عادل عبد صادق، أسلحة الفضاء الالكتروني في ضوء القانون الدولي الإنساني، مرجع سابق، ص136.

(29) حامد محمد علي البلداوي، الهجمات السيبرانية أضرارها وآثارها ومواجهاتها في قواعد القانون الدولي الإنساني، المركز العربي، القاهرة، 2024، ص133.

(30) أحمد سعد محمد الحسيني، الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية، أطروحة أعدت لنيل درجة الدكتوراه في القانون العام، جامعة عين شمس، كلية الحقوق، مصر، 2012، ص 279.

[31] درار نسيمة، الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الالكتروني، أطروحة اعدت لنيل درجة الدكتوراه في القانون العام، جامعة أبو بكر، كلية الحقوق، الجزائر، 2017، ص 76.

[32] عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الإسكندرية، مصر، 2015، ص 24-25.

[33] عبد الحميد ابراهيم العربان، العلاقة بين الإرهاب المعلوماتي والجرائم المنظمة، بحث منشور على الموقع الإلكتروني
التالي:
http://nauss.edu.sa/bitstream/handle/123456%D8%A7%D9%85.pdf?sequence=1%E2%80%8F،
تاريخ الزيارة 2024/11/15.

[34] محمود الحمدان، الإرهاب الإلكتروني وسبل المواجهة، المرجع الإلكتروني السابق، ص 5.

[35] محمد أمين الرومي، جرائم الكمبيوتر والإنترنت دار المطبوعات الجامعية، الإسكندرية، مصر، 2018، ص237.

[36] حامد محمد علي البلداوي، مرجع سابق، ص137.

[37] ناصر العماش، الملتقى الوطني للأمن السيبراني، مقال منشور على الموقع الإلكتروني التالي: https://www.alriyadh.com/2003607 ، تاريخ الزيارة 2024/11/16.

[38] **جمال إبراهيم الحيدري، الجرائم الإلكترونية وسبل مواجهتها، مرجع سابق، ص 130.**

[39] أحمد عبيس نعمة الفتلاوي، مشكلة الأسلحة التقليدية بين جهود المجتمع الدولي والقانون الدولي العام، دار النهضة العربية، مصر، 2018، ص 31.

[40] الأمم المتحدة، تحذير أممي من مخاطر الاستخدام غير المسؤول للتكنولوجيات الحديثة على الأمن البشري والدولي، تقرير منشور على الرابط التالي https://news.un.org/ar/story/2024/10/1135866، تاريخ الزيارة 2025-1-15.

[41] نورة شلوش، القرصنة الإلكترونية في الفضاء السيبراني، التهديد المتصاعد لأمن الدول، بحث منشور في مجلة مركز بابل للدراسات الإنسانية، العدد 6، المجلد 8، جامعة بابل، العراق، 2018، ص 190.

[42] كاميران عزيز حسن، الجهود الدولية في مواجهة الجرائم السيبرانية، ط1، منشورات الحلبي الحقوقية، لبنان، 2021، ص29.

[43] خالد وليد محمود، الهجمات عبر الانترنت ساحة الصراع الالكتروني الجديدة، المركز العربي للأبحاث ودراسة السياسات، الدوحة، 2013، ص 44.

[44] دليل تالين Manuel de Tallinn) هو وثيقة قانونية أعدها مجموعة من الخبراء تحت إشراف منظمة حلف شمال الأطلسي (OTAN) وبمساعدة اللجنة الدولية للصليب الاحمر (CICR) تتضمن قواعد القانون الدولي المطبقة أثناء الحروب السيبرية.

[45] منير البعلبكي، المورد قاموس عربي-انكليزي، دار العلم للملايين، بيروت، 2004، ص 243.

[46] عادل موسى عوض جاب الله، وسائل حماية الأمن السيبراني دراسة فقهية تأصيلية مقارنة بالنظم المعاصرة، كلية الشريعة والدراسات الإسلامية، مصر، 2022، ص20.

[47] حسين محمد الغول، جرائم شبكة الانترنت والمسؤولية الجزائية الناشئة عنها، منشورات زين الحقوقية، بيروت، 2017، ص46-47.

[48] المادة (51) من ميثاق الأمم عام 1945.

[49] على فاضل على سليمان، حق الدفاع الشرعي على الهجمات السيبرانية، بحث منشور بمجلة تكريت للحقوق، المجلد رقم (4)، العدد رقم (4)، العراق، 2020، ص 254.

[50] محمد علي كنده فلاح، الحرب السيبرانية وتهديد الأمن القومي لجمهورية الإسلامية، أطروحة أعدت لنيل درجة الدكتوراه، جامعة آزاد إسلامي، كلية الآداب والعلوم الإنسانية، قم، إيران، 2012.

[51] المادة (48) من الملحق الإضافي لاتفاقية جنيف والتي نصت على (تعمل أطراف النزاع على التمييز بين السكان المدنيين والمقاتلين وبين الأعيان المدنية والأهداف العسكرية، ومن ثم توجه عملياتها ضد الأهداف العسكرية دون غيرها، وذلك من أجل تأمين احترام وحماية السكان المدنيين والأعيان المدنية).

[52] سليم عبد الله الجبوري، الحماية القانونية لمعلومات شبكة الإنترنت، منشورات الحلبي الحقوقية، لبنان، 2011، ص 25.

[53] هدى ميتكيس وصدقي عابدين، قضايا الأمن في آسيا، مركز الدراسات الاسيوية، جامعة القاهرة، مصر، 2016، ص 114.

قائمة المصادر والمراجع

أولاً_ الكتب القانونية

1. إسماعيل محمود الرزاز، الحماية القانونية من الهجمات والجرائم السيبرانية، مركز المحمود لتوزيع الكتب القانونية، مصر، 2023.
2. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية، ط1، منشورات زين الحقوقية، بيروت، 2018.
3. عادل عبد صادق، أسلحة الفضاء الالكتروني في ضوء القانون الدولي الإنساني، مكتبة الإسكندرية، الإسكندرية، 2016.
4. عبد الكريم الردايدة، الجرائم المستحدثة واستراتيجية مواجهتها، الطبعة الأولى، منشورات دار حامد للنشر والتوزيع، عمان، الأردن، 2013.
5. علي محمد كاظم الموسوي، المشاركة المباشرة في الهجمات السيبرانية، المؤسسة الحديثة للكتاب، بيروت، 2019.
6. جمال إبراهيم الحيدري، الجرائم الإلكترونية وسبل معالجتها، منشورات مكتبة السنهوري، بغداد، 2012.

7. تميم عبد الله التميمي، الجرائم المعلوماتية في الاعتداء على الأشخاص، الطبعة الأولى، منشورات مكتبة القانون والاقتصاد، الرياض، 2016.
8. طارق إبراهيم الدسوقي عطية، عولمة الجريمة، الشركات العالمية في الممارسات الإجرامية، دار الجامعة الجديدة، الإسكندرية، مصر، 2010.
9. جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، 2012.
10. جلال محمد الزغبي وأسامة أحمد المناعسة، جرائم تقنية المعلومات الإلكترونية، الطبعة الأولى، منشورات دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010.
11. حامد محمد علي البلداوي، الهجمات السيبرانية أضرارها وآثارها ومواجهاتها في قواعد القانون الدولي الإنساني، المركز العربي، القاهرة، 2024.
12. عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الإسكندرية، مصر، 2015.
13. أحمد عبيس نعمة الفتلاوي، مشكلة الأسلحة التقليدية بين جهود المجتمع الدولي والقانون الدولي العام، در النهضة العربية، مصر، 2018.
14. كاميران عزيز حسن، الجهود الدولية في مواجهة الجرائم السيبرانية، ط1، منشورات الحلبي الحقوقية، لبنان، 2021.
15. خالد وليد محمود، الهجمات عبر الانترنت ساحة الصراع الالكتروني الجديدة، المركز العربي للأبحاث ودراسة السياسات، الدوحة، 2013.
16. منير البعلبكي، المورد قاموس عربي-انكليزي، دار العلم للملايين، بيروت، 2004.
17. عادل موسى عوض جاب الله، وسائل حماية الأمن السيبراني دراسة فقهية تأصيلية مقارنة بالنظم المعاصرة، كلية الشريعة والدراسات الإسلامية، مصر، 2022.
18. حسين محمد الغول، جرائم شبكة الانترنت والمسؤولية الجزائية الناشئة عنها، منشورات زين الحقوقية، بيروت، 2017.
19. سليم عبد الله الجبوري، الحماية القانونية لمعلومات شبكة الإنترنت، منشورات الحلبي الحقوقية، لبنان، 2011.
20. هدى ميتكيس وصدقي عابدين، قضايا الأمن في آسيا، مركز الدراسات الاسيوية، جامعة القاهرة، مصر، 2016.

ثانياً_ المجلات والدوريات

1. ذياب موسى البداينة، الجرائم المستحدثة في ظل المتغيرات التحولات الإقليمية والدولية، بحث مقدم إلى الملتقى العملي في كلية العلوم الاستراتيجية، عمان، الأردن، 2014.
2. طارق عثمان، المركز الوطني للاستجابة لطوارئ الحاسب الآلي، صحيفة الدستور، العدد 12، مصر، 2012.
3. نورة شلوش، القرصنة الإلكترونية في الفضاء السيبراني، التهديد المتصاعد لأمن الدول، بحث منشور في مجلة مركز بابل للدراسات الإنسانية، العدد 6، المجلد 8، جامعة بابل، العراق، 2018.
4. على فاضل على سليمان، حق الدفاع الشرعي على الهجمات السيبرانية، بحث منشور بمجلة تكريت للحقوق، المجلد رقم (4)، العدد رقم (4)، العراق، 2020.
5. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، كلية القانون، جامعة بابل، العدد 4، العراق، 2016.

ثالثاً_ الأطاريح

1. زهراء عماد محمد، المسؤولية الدولية الناشئة عن الهجمات السيبرانية، مكتبة القانون المقارن، العراق، 2021.
2. محمود ابراهيم عبد الرحمن، أسلحة غير التقليدية في الفقه الإسلامي، أطروحة دكتوراه، كلية الشريعة والقانون، الجامعة الإسلامية، غزة، 2007.
3. رايز بن سالم الحقباني، مهارات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه مقدمة إلى جامعة نايف للعلوم الأمنية، الرياض، 2013.
4. أحمد سعد محمد الحسيني، الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية، أطروحة أعدت لنيل درجة الدكتوراه في القانون العام، جامعة عين شمس، كلية الحقوق، مصر، 2012.
5. محمد علي كنده فلاح، الحرب السيبرانية وتهديد الأمن القومي لجمهورية الإسلامية، أطروحة أعدت لنيل درجة الدكتوراه، جامعة آزاد إسلامي، كلية الآداب والعلوم الإنسانية، قم، إيران، 2012.
6. درار نسيمة، الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الالكتروني، أطروحة اعدت لنيل درجة الدكتوراه في القانون العام، جامعة أبو بكر، كلية الحقوق، الجزائر، 2017.

رابعاً_ المواثيق والاتفاقيات الدولية

1. البروتوكولان الإضافيان إلى اتفاقية جنيف لعام 1949.

2. ميثاق الأمم عام 1945.

خامساً_ المصادر الالكترونية

1. عبد الحميد ابراهيم العربان، العلاقة بين الإرهاب المعلوماتي والجرائم المنظمة، بحث منشور على الموقع الإلكتروني التالي

، تاريخ الزيارة http://nauss.edu.sa/bitstream/handle/123456%D8%A7%D9%85.pdf?sequence=1%E2%80%8F:

.2024/11/15

2. ناصر العماش، الملتقى الوطني للأمن السيبراني، مقال منشور على الموقع الإلكتروني التالي: https://www.alriyadh.com/2003607 ، تاريخ الزيارة 2024/11/16.

المصادر والمراجع العربية باللغة الانكليزية

Firstly, legal books

1 .Ismail Mahmoud Al-Razzaz, Legal Protection from Cyberattacks and Crimes, Al-Mahmoud Center for Distributing Legal Books, Egypt, 2023.

2 .Ahmed Abis Nima Al-Fatlawi, Cyber Attacks, 1st edition, Zain Human Rights Publications, Beirut, 2018.

3 .Adel Abdel Sadiq, Cyber Weapons in Light of International Humanitarian Law, Bibliotheca Alexandria, Alexandria, 2016.

4. Abdul Karim Al-Radaida, New Crimes and the Strategy to Confront Them, first edition, Dar Hamed Publishing and Distribution Publications, Amman, Jordan, 2013.

5 .Jamal Ibrahim Al-Haidari, Cybercrimes and Ways to Address them, Al-Sanhouri Library Publications, Baghdad, 2012.

6 .Tamim Abdullah Al-Tamimi, Information Crimes in Assault on Persons, first edition, Publications of the Library of Law and Economics, Riyadh, 2016.

. Tariq Ibrahim Al-Desouki Attia, The Globalization of Crime, International Companies in Criminal Practices, New University House, Alexandria, Egypt, 2010.

8 .Jamil Abdel Baqi Al-Saghir, Procedural Aspects of Internet-Related Crimes, Dar Al-Nahda Al-Arabiya, Cairo, 2012.

9 .Jalal Muhammad Al-Zoghbi and Osama Ahmed Al-Manasa, Electronic Information Technology

Crimes, first edition, Dar Al-Thaqafa Publishing and Distribution Publications, Amman, Jordan, 2010.

10 .Hamed Muhammad Ali Al-Baldawi, Cyberattacks, Their Harms, Effects, and Confrontations in the Rules of International Humanitarian Law, the Arab Center, Cairo, 2024.

Second: Magazines and periodicals

Dhiyab Musa Al-Badaina**,** New Crimes in Light of Regional and International Changes, research presented to the practical forum at the College of Strategic Sciences, Amman, Jordan, 2014.

2. Tariq Othman, National Center for Computer Emergency Response, Al-Dustour newspaper, issue 12, Egypt, 2012.

3. Noura Shaloush, Electronic piracy in cyberspace, the rising threat to the security of countries, research published in the Journal of the Babylon Center for Humanitarian Studies, Issue 6, Volume 8, University of Babylon, Iraq, 2018.

4. Ali Fadel Ali Suleiman, The Right to Legal Defense Against Cyber Attacks, research published in Tikrit Law Journal, Volume No. (4), Issue No. (4), Iraq, 2020.

Third: Theses

1. Zahraa Imad Muhammad, International Liability Arising from Cyber Attacks, Comparative Law Library, Iraq, 2021.

2. Mahmoud Ibrahim Abdel Rahman, Unconventional Weapons in Islamic Jurisprudence, PhD thesis, Faculty of Sharia and Law, Islamic University, Gaza, 2007.

3. Rayez bin Salem Al-Haqbani, Research and Investigation Skills in Information Crimes, doctoral thesis submitted to Naif University for Security Sciences, Riyadh, 2013.

4 .Ahmed Saad Muhammad Al-Husseini, Procedural Aspects of Crimes Arising from the Use of Electronic Networks, a thesis prepared to obtain a doctorate degree in public law, Ain Shams University, Faculty of Law, Egypt, 2012.

5. Muhammad Ali Kindeh Falah, Cyberwar and the Threat to the National Security of the Islamic Republic, a thesis prepared for the doctoral degree, Azad Islami University, Faculty of Arts and Humanities, Qom, Iran, 2012.

Darar Nassima, Information Security and Ways to Confront Its Risks in Electronic Transactions, a thesis prepared to obtain a doctorate degree in public law, Abu Bakr University, Faculty of Law, Algeria, 2017.

Fourth: International charters and agreements

1. The Two Additional Protocols to the Geneva Convention of 1949.

2. The Charter of Nations in 1945.

Fifth: Electronic sources

1. Abdul Hamid Ibrahim Al-Arban, the relationship between cyber terrorism and organized crimes, research published on the following website: http://nauss.edu.sa/bitstream/handle/123456%D8%A7%D9%85.pdf?sequence=1%E2%80%8F, date of visit 11/15/2024.

2. Nasser Al-Ammash, National Cybersecurity Forum, article published on the following website: https://www.alriyadh.com/2003607, date of visit: 11/16/2024.

International responsibility for cybercrimes and ways to address them in international law

Dr. Essam Ali Hussein

College of Law-Al-Amin University

akelalaa04@gmail.com

Keywords: Cyber crimes . international mechanisms . international responsibility.

Summary:

Confronting cybercrime requires an integrated and comprehensive international effort that includes developing laws, enhancing cooperation, and investing in building technical and legal capabilities. Although the road is long and complex, formulating sustainable legal solutions will contribute to protecting international security and ensuring justice for all parties affected by these crimes. Achieving a balance between protecting privacy and national sovereignty on the one hand, and enhancing global cybersecurity on the other hand, remains the greatest challenge that the international community must face with wisdom and precision.